



## Cisco Cloud APIC への既存のブラウンフィールド AWS クラウド VPC のインポート

[新機能および変更された機能に関する情報 2](#)

[Cisco Cloud APIC への既存のブラウンフィールド AWS クラウド VPC のインポートの利点 2](#)

[このドキュメントで使用される用語 5](#)

[アンマネージド \(ブラウンフィールド\) VPC のトランジット ゲートウェイ アタッチメントについて 5](#)

[ブラウンフィールド VPC でできることとできないこと Cisco Cloud APIC 6](#)

[注意事項および制約事項 7](#)

[既存のブラウンフィールドクラウド VPC を Cisco Cloud APIC にインポートするためのワークフロー 8](#)

[読み取り専用アカウントの設定 9](#)

[管理対象外 \(ブラウンフィールド\) クラウド コンテキスト プロファイルの作成 12](#)

[AWS でのアンマネージド VPC のトランジット ゲートウェイ アタッチメントの追加 19](#)

[ブラウンフィールドクラウドコンテキスト プロファイルに関連付けられた EPG の作成 20](#)

[AWS でのブラウンフィールド VPC の残りの構成の完了 29](#)

改訂：2022年4月6日、

## 新機能および変更された機能に関する情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

Cisco APIC のリリース バージョン	特長	説明
25.0(2)	Cisco Cloud APIC への既存のブラウフィールド AWS クラウド VPC のインポートのサポート	このリリースでは、既存のブラウフィールド AWS クラウド VPC を Cisco Cloud APIC に指定します。

## Cisco Cloud APIC への既存のブラウフィールド AWS クラウド VPC のインポートの利点



- (注)
- このドキュメントでは、ブラウフィールド VPC は、Cisco Cloud APIC の介入なしにユーザーが作成する VPC として定義されています。リリース 25.0(2) でのこの初期サポートでは、ブラウフィールド VPC とアンマネージド VPC は同じことを意味します。
  - このドキュメントでは、特に、既存のブラウフィールド AWS クラウド VPC のインポートについて説明します。これは、リリース 25.0(2) 以降でサポートされます。Cisco Cloud APIC リリース 5.2(1) からサポートされていた既存のブラウフィールド Azure クラウド VNet のインポートについては、「既存のブラウフィールド Azure クラウド VNet を Cisco Cloud APIC にインポートする」を参照してください。Cisco Cloud APIC

リリース 25.0(2) より前では、Cisco Cloud APIC を通じたクラウド導入はグリーンフィールド導入と見なされ、必要なコンポーネント（リソース グループ、VPC、CIDR、サブネットなど）の設定は Cisco Cloud APIC を通じて行われます。次に、Cisco Cloud APIC で作成したこれらのリソース グループの下にサービスを展開し、アプリケーションを起動します。

データセンター拡張に Amazon Web Services (AWS) を採用した多くのユーザーは、すでにクラウドに導入された数百の VPC とインスタンスを持っています。これにより、AWS の Cisco Cloud APIC を通じた新しいグリーンフィールド設定と既存のブラウフィールド設定の2つの異なる環境ができます。Cisco Cloud APIC ソリューションを導入した後、既存のクラウドリソースに個別のコントロール ポイントが必要ない場合、これは理想的ではありません。

リリース 25.0(2) よりも前では、リソース グループと VPC が Cisco Cloud APIC を使用せずに作成された既存のブラウフィールド環境は、Cisco Cloud APIC のマネージド サイトで共存できませんでした。リリース 25.0(2) 以降では、既存のブラウフィールド AWS VPC を Cisco Cloud APIC にインポートできるようになりました。この拡張機能では、AWS トランジット ゲートウェイを使用して、Cisco Cloud APIC を通じて設定されたグリーンフィールド VPC と Cisco Cloud APIC の外部で設定されたブラウフィールド VPC 間の通信を提供します。

次の図は、AWS トランジット ゲートウェイが構成されているか、AWS トランジット ゲートウェイ接続が構成されている AWS トポロジの例を示しています。Cisco Cloud APIC および AWS トランジット ゲートウェイまたはトランジット ゲートウェイの接続の詳細については、ドキュメント「AWS トランジット ゲートウェイまたは AWS トランジット ゲートウェイ コネクトを使用した VPC 間の帯域幅の増加」を参照してください。

図 1: AWS トランジット ゲートウェイを使用した AWS トポロジの例

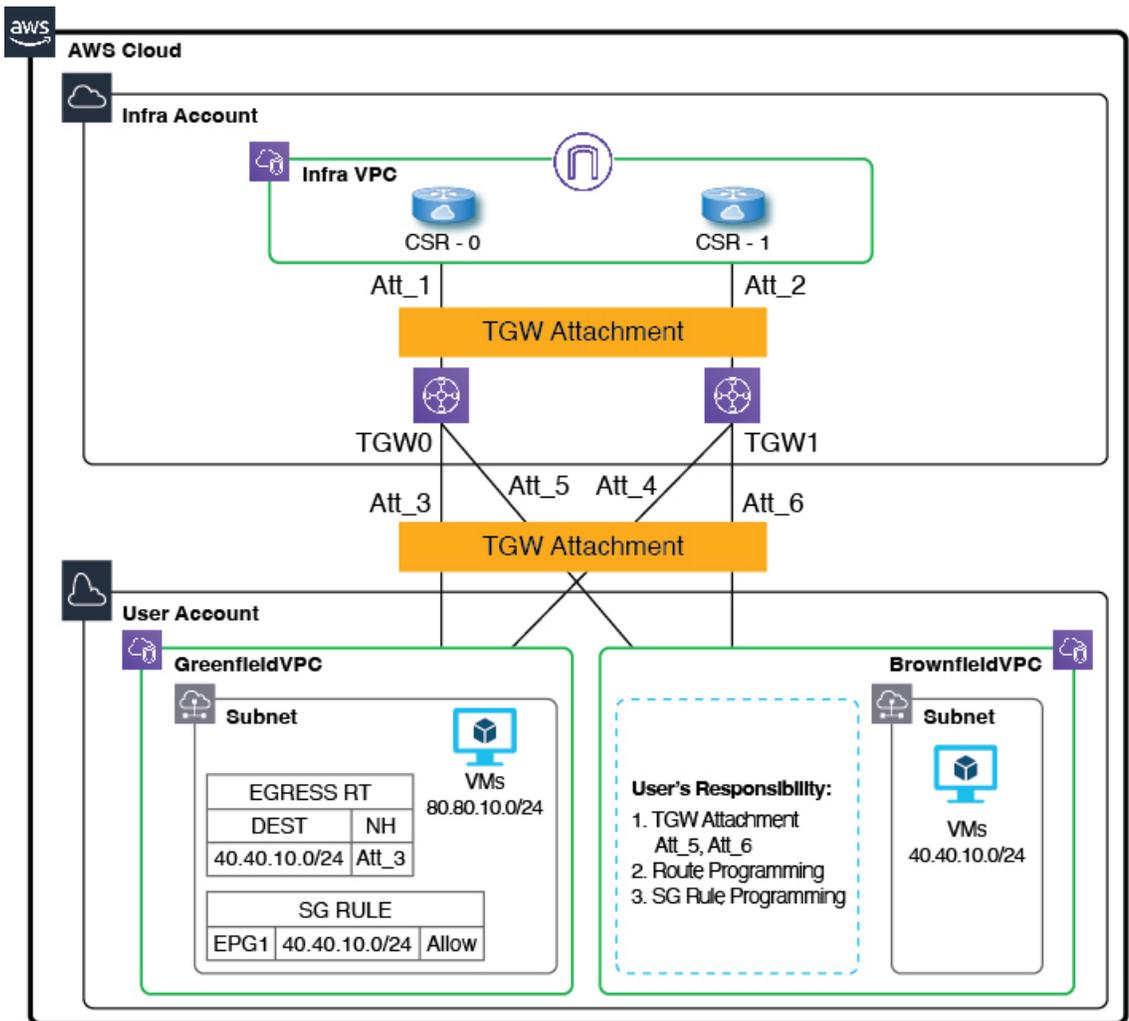
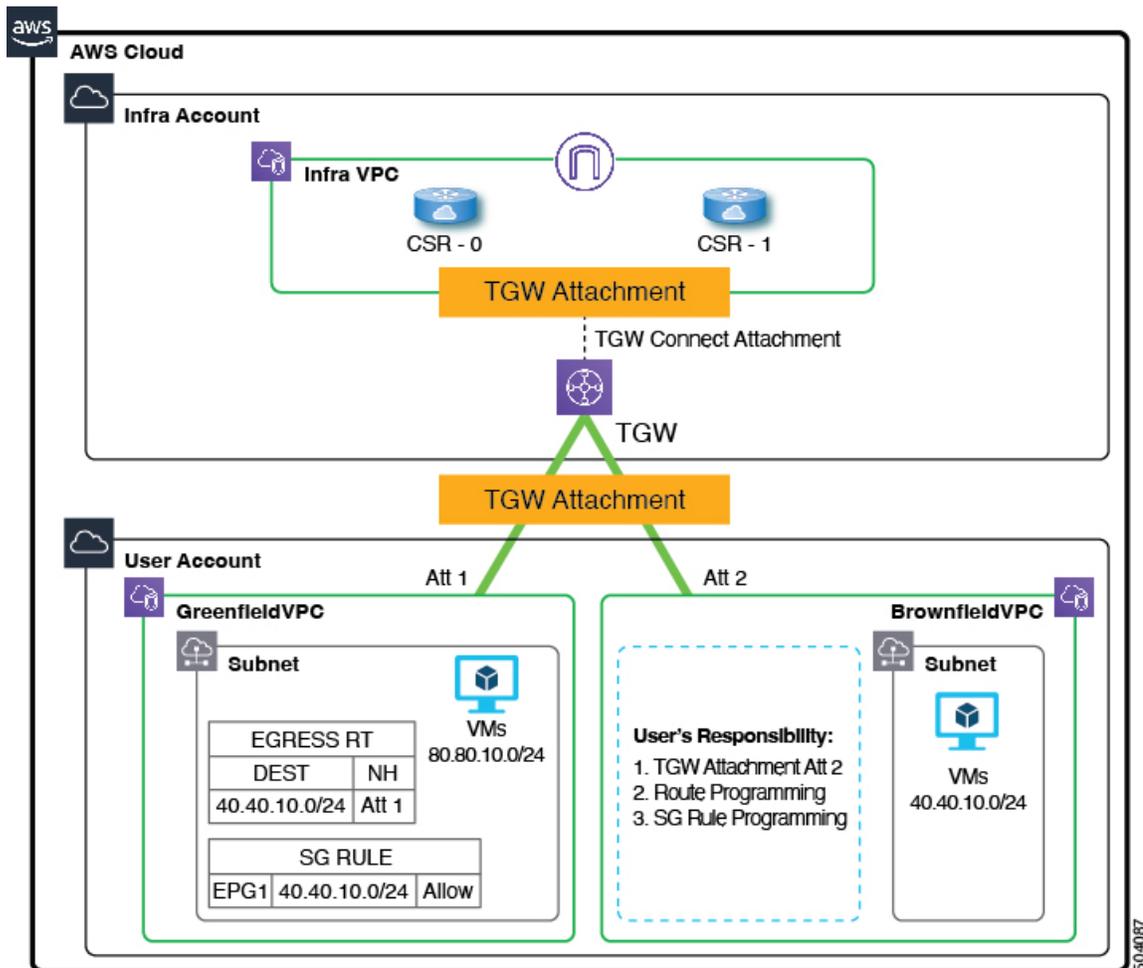


図 2: AWS トランジット ゲートウェイ コネクトを使用した AWS トポロジの例



上の図では、次のように設定されています。

- インフラ VPC とグリーンフィールド VPC が作成され、Cisco Cloud APIC を通じて管理されています。さらに、グリーンフィールド VPC の場合、トランジット ゲートウェイ アタッチメントは Cisco Cloud APIC によって作成されます。
- ブラウンフィールド VPC は AWS 経由で作成され、Cisco Cloud APIC の外部で管理されます。さらに、リリース 25.0(2) では、ブラウンフィールド VPC は読み取り専用アカウントでのみインポートできるため、Cisco Cloud APIC はトランジット ゲートウェイ アタッチメントを作成する権限はありません。この場合、ネットワークが完成するように、トランジット ゲートウェイ アタッチメントを手動で作成する必要があります。詳細については、「[読み取り専用アカウントの概要 \(9 ページ\)](#)」を参照してください。

この機能を使用すると、Cisco Cloud APIC は既存のブラウンフィールドリソースグループで何も設定またはプロビジョニングされないことに注意してください。セキュリティグループルール、ルートテーブル、およびルータは、これらのブラウンフィールドリソースグループでは Cisco Cloud APIC を通じてプログラムされません。Cisco Cloud APIC は、これらの既存のブラウンフィールド展開のセキュリティグループルール、ルートテーブルおよびルータを管理しない

ため、Cisco Cloud APIC の外部の既存のブラウンフィールド展開のセキュリティ グループ ルール、ルート テーブルおよびルートを引き続き管理します。

さらに、Cisco Cloud APIC (CIDR、サブネット、ルート テーブル、トランジット ゲートウェイ、トランジット ゲートウェイ VPC アタッチメントなど) にインポートしたくないブラウンフィールド VPC の下に既存のクラウドリソースがある場合、これらの既存のクラウドリソースは Cisco Cloud APIC から変更または削除されることなく引き続き存在し続けます。読み取り専用アクセスポリシーでは、読み取りインベントリの実行を除き、Cisco Cloud APIC はこれらの既存のクラウドリソースに対する権限はありません。

## このドキュメントで使用される用語

このセクションでは、このドキュメントで使用される主要な用語と概念の一部を紹介します。

### グリーンフィールド VPC

クラウド コンテキスト プロファイルの Cloud APIC に基づいて作成される AWS 上の VPC。

### ブラウンフィールドまたはアンマネージド VPC

ポリシーを使用せずに作成された AWS の VPC。Cloud APIC

### アクセス ポリシー

Cloud APIC で作成されたポリシーは、それぞれの権限を示します。現在、ポリシーは次のとおりです。

- デフォルト
- 読み取り専用
- Unmanaged

### 読み取り専用クラウド コンテキスト プロファイル

読み取り専用アクセス ポリシーに関連するクラウド コンテキスト プロファイル。

### 読み取り専用アカウント

読み取り専用アクセス ポリシーに関連するクラウド アカウント。読み取り / 書き込みアカウントも使用できますが、読み取り / 書き込みアカウントは読み取り専用アクセス ポリシーとは関係がないことに注意してください。

### グリーンフィールドクラウド コンテキスト プロファイル

アクセス ポリシーと関係がない、またはデフォルト アクセス ポリシーと関係がないクラウド コンテキスト プロファイル。

## アンマネージド (ブラウンフィールド) VPC のトランジット ゲートウェイ アタッチメントについて

通常、AWS トランジットゲートウェイ構成の一部としてクラウド上にグリーンフィールドVPCを作成すると、グリーンフィールド VPC とトランジット ゲートウェイ間のトランジットゲートウェイのアタッチメントも構成されます。

### Cisco Cloud APIC

ただし、アンマネージド (ブラウンフィールド) VPC で AWS トランジットゲートウェイを構成する場合、Cisco Cloud APIC はブラウンフィールド VPC とインフラ トランジットゲートウェイ間のトランジットゲートウェイアタッチメントを構成できないため、ブラウンフィールドVPCのトランジットゲートウェイアタッチメント構成は使用者が手動で行う必要があります。

グリーンフィールド VPC とブラウンフィールド VPC の間で通信を行うには、ブラウンフィールド VPC のトランジット ゲートウェイ アタッチメントをグリーンフィールド トランジット ゲートウェイ (Cisco Cloud APIC によって作成された TGW) に手動で設定する必要があります。これがないと、グリーンフィールド VPC とブラウンフィールド VPC の間でパケット フローが発生しません。

詳細については、ドキュメント「AWS トランジット ゲートウェイまたは AWS トランジット ゲートウェイ コネクトを使用した VPC 間の帯域幅の増加」を参照してください。 <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/cloud-apic/5-x/use-case/increasing-bandwidth-using-aws-transit-gateway-or-aws-transit-gateway-connect.html>

## ブラウンフィールド VPC でできることとできないこと Cisco Cloud APIC

リリース 25.0(2) の一部としてのこの拡張により、Cisco Cloud APIC はブラウンフィールド VPC とパケットを送受信できるように、グリーンフィールド リソース グループ/VPC 側で必要なネットワーク接続とセキュリティを調整できます。

ブラウンフィールド VPC を Cisco Cloud APIC で登録すると、次の設定が行われます。

- インベントリ プルは、ブラウンフィールド リソース グループまたは VPC で実行されます。
- ブラウンフィールド クラウド EPG とグリーンフィールド クラウド EPG の間のコントラクトに基づいて、特定のエリアでのみ必要な設定を行います。Cisco Cloud APIC
  - グリーンフィールド VPC のセキュリティ グループ ルールをプログラムして、ブラウンフィールド VPC との間のインバウンドおよびアウトバウンド トラフィックを許可します。ブラウンフィールド VPC のセキュリティ グループ ルールをプログラムしません。Cisco Cloud APIC Cisco Cloud APIC ブラウンフィールド VPC のセキュリティ グループ ルールを個別に手動でプログラムする必要があります。
  - Cisco Cloud APIC ブラウンフィールド VPC のルート テーブルまたはルートをプログラミングしません。ブラウンフィールド VPC がグリーンフィールド VPC と通信するには、次の構成を手動で行う必要があります。
    - グリーンフィールドとブラウンフィールドの EPG 間のコントラクトを作成します。
    - インフラ トランジット ゲートウェイを使用してトランジット ゲートウェイ VPC アタッチメントを作成する
    - ブラウンフィールド VPC とサブネットのルート テーブルを作成します。
    - 宛先がグリーンフィールド CIDR であり、ネクストホップがトランジット ゲートウェイ VPC アタッチメントであるルートを追加します
- すべての CSR にブラウンフィールド VPC に対応する VRF を作成し、ブラウンフィールド VPC の CIDR に対応するアクセス制御リストとルートを作成します。また、構成されたコントラクトに基づいて、CSR でルート リークを構成します。Cisco Cloud APIC Cisco Cloud APIC
- Cisco Cloud APIC ブラウンフィールド VPC の作成に使用された AWS アカウントにインフラ トランジット ゲートウェイを共有します。この時点で、ブラウンフィールド VPC のインポートを続行する前に、トランジット ゲートウェイ VPC アタッチメントを手動で作成する必要があります。Cisco Cloud APIC

VRF を介したブラウフィールドクラウドコンテキストプロファイルに関連付けられているクラウド EPG には、サブネットベースのエンドポイントセレクタが必要です（タグベースの EPG はブラウフィールドクラウドコンテキストプロファイルには適用されません）。

Cisco Cloud APIC ルートプログラミングの構成、セキュリティグループルールの作成、またはトランジットゲートウェイ VPC アタッチメントの作成など、ブラウフィールド VPC に関してクラウドリソースを作成しません。

さらに、ブラウフィールド VPC を Cisco Cloud APIC に登録すると、次の Cisco Cloud APIC コンポーネントが影響を受けるか、影響を受けません。

- ブラウフィールド VRF の CSR プログラミングに変更はありません。CSR の観点からは、ブラウフィールド VRF は他の VRF と同様に動作します。CSR では、ブラウフィールド VRF はブラウフィールドクラウドコンテキストプロファイルの一部としてインポートされた CIDR とともにプログラムされます。CSR は、特定の VRF がグリーンフィールドまたはブラウフィールドクラウドコンテキストプロファイルに関連付けられているかどうかを認識していません。
- アクセス制御リストは GigabitEthernet1 インターフェイスでプログラムされることにより、これらのアンマネージド（ブラウフィールド）VPC CIDR とのトラフィックの行き来を許可します。コントラクトに基づいて、VRF に関連付けられた EPG 間でルートリークが発生します。

## 注意事項および制約事項

次に、既存のブラウフィールドクラウド設定を Cloud APIC にインポートする際の注意事項と制約事項を示します。

- アンマネージド（ブラウフィールド）クラウドコンテキストプロファイルには、特に次の注意事項と制約事項が適用されます。
  - アンマネージド VPC の特定の VPC ID は、Cisco Cloud APIC 上の 2 つの異なるアンマネージドクラウドコンテキストプロファイルにマッピングできません。特定の VPC ID は、Cisco Cloud APIC で 1 つのアンマネージドクラウドコンテキストプロファイルのみを作成するために使用できます。
  - クラウドコンテキストプロファイルにマッピングされたアンマネージド VPC は、このクラウドコンテキストプロファイルに関連付けられているテナントと同じ AWS アカウントに存在する必要があります。Cisco Cloud APIC でこれらのアンマネージドクラウドコンテキストプロファイルを定義している間は、ランダムな VPC ID を指定できません。
  - リージョンは、ブラウフィールド VPC が作成されたものと同じである必要があります。
  - CIDR は、ブラウフィールド VPC で構成されたものと同じである必要があります。
  - ブラウフィールド VPC の下で CIDRS のすべてまたは特定のセットを選択的にインポートできますが、プライマリ CIDR がなければブラウフィールド VPC をインポートすることはできません。ブラウフィールド VPC をインポートする場合、プライマリ CIDR のインポートは必須です。
- ホスト VRF は、ブラウフィールド VPC のインポートには使用できません。

# 既存のブラウフィールドクラウド VPC を Cisco Cloud APIC にインポートするためのワークフロー

以下は、グリーンフィールド VPC (Cisco Cloud APICによって構成および管理される VPC) がブラウフィールド VPC (Cisco Cloud APICで管理されない VPC) との間でトラフィックを送受信するための一般的なワークフローです。

1. ブラウフィールド (アンマネージド) VPC が AWS ですでに作成されていることを確認します。
2. このブラウフィールド (アンマネージド) VPC を Cisco Cloud APIC にインポートします。
  1. 必要な場合は、アンマネージド (ブラウフィールド) クラウド コンテキスト プロファイルで使用する新しいテナントを作成します。

ブラウフィールド VPC は、同じ AWS アカウントに存在することも、グリーンフィールド VPC とは異なる AWS アカウントに存在することもあります。

ブラウフィールド VPC が別の AWS アカウントにある場合は、このアカウントを指す AWS アカウント ID フィールド (cloudAwsProvider) フィールドで新しいテナントを作成する必要があります。この AWS アカウントがブラウフィールド VPC の管理にのみ使用される場合、このテナントは「読み取り専用」アクセスポリシーに関連します。この読み取り専用ポリシーは、イベントと統計タスクがトリガーされず、フローログがこのアカウントで構成されないことを意味します。このアカウントでは、インベントリ プルのみが実行されます。詳細については、「[読み取り専用アカウントの概要 \(9 ページ\)](#)」を参照してください。

新しいテナントを作成する手順については、[読み取り専用アカウントの設定 \(9 ページ\)](#) または、『Cisco Cloud APIC for AWS User Guide』、リリース 25.0(x) 以降の「リリース 4.2(3) およびそれ以降向けテナント AWS プロバイダーの構成」を参照してください。<https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/series.html>

2. Cisco Cloud APIC に既存のブラウフィールド VPC、CIDR、およびサブネット設定をインポートします。

これを行うには、ブラウフィールド VPC に対応するクラウド コンテキスト プロファイルを作成します。これにより、ブラウフィールド VPC と VRF の間に関連付けが作成されます。Cisco Cloud APIC のクラウド コンテキスト プロファイルは、ブラウフィールド VPC と VRF 間のリンクに使用されるオブジェクトです。ブラウフィールド VPC をインポートするには、最初に VRF オブジェクトを作成する必要があります。これは、後でブラウフィールド VPC をインポートするときに使用されるクラウド コンテキスト プロファイル関連付けのプレースホルダです。

これらの手順については、[管理対象外 \(ブラウフィールド\) クラウド コンテキスト プロファイルの作成 \(12 ページ\)](#) を参照してください。

3. AWS のアンマネージド (ブラウフィールド) VPC のトランジット ゲートウェイ アタッチメントを追加します。

Cisco Cloud APIC はアンマネージド (ブラウフィールド) VPC と AWS のインフラ トランジット ゲートウェイ (Cisco Cloud APIC によって作成された TGW) との間に AWS トランジット ゲートウェイ アタッチメントを構成しません。インフラ構成の一部として作成された AWS トランジット ゲートウェイはブラウフィールド ユーザー アカウントと共有されますが、アンマネージド (ブラウフィールド) VPC と AWS のインフラ トランジット ゲートウェイ間の AWS トランジット ゲートウェイ アタッチメントを手動で構成する必要があります。

詳細については、「[AWS でのアンマネージド VPC のトランジット ゲートウェイ アタッチメントの追加 \(19 ページ\)](#)」を参照してください。

4. この VRF の下にクラウド EPG を作成し、グリーンフィールド EPG に対するコントラクトを構成します。

これらの手順については、[ブラウンフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成 \(20 ページ\)](#) を参照してください。

ブラウンフィールド (アンマネージド) VPC を Cisco Cloud APIC にインポートする場合：

- ブラウンフィールドクラウド EPG とグリーンフィールドクラウド EPG 間のコントラクトに基づいて、グリーンフィールド VPC のルートテーブルとセキュリティグループルールをプログラムします。Cisco Cloud APIC
  - すべての CSR にブラウンフィールド VPC に対応する VRF を作成し、ブラウンフィールド VPC の CIDR に対応するアクセス制御リストとルートを作成します。また、構成されたコントラクトに基づいて、CSR でルートリークを構成します。Cisco Cloud APIC
  - Cisco Cloud APIC ルートプログラミングの構成、セキュリティグループルールの作成、またはトランジットゲートウェイ VPC アタッチメントの作成など、ブラウンフィールド VPC に関してクラウドリソースを作成しません。
5. Cisco Cloud APIC トランジットゲートウェイルートテーブルを関連付け、ブラウンフィールドトランジットゲートウェイ VPC アタッチメントの伝播を構成します。ただし、Cisco Cloud APIC はブラウンフィールド VPC のセキュリティグループルールプログラミングを構成しないため、AWS ポータルから手動でこれらの構成を行う必要があります。

## 読み取り専用アカウントの設定

次のセクションでは、読み取り専用アカウントの設定に関して説明します。

### 読み取り専用アカウントの概要



---

(注) リリース 25.0(2) では、ブラウンフィールド VPC は、このセクションで説明されている読み取り専用アカウントにのみインポートできます。

---

アンマネージド VPC のみを含むアカウントがあり、AWS でこのアカウントの VPC を管理するために Cisco Cloud APIC を使用しない場合は、このアカウントを読み取り専用アカウントとして定義できます。読み取り専用アカウント (ポリシー) は、これらのアカウントでイベント収集 / 統計収集リソースの作成をトリガーしません。この読み取り専用ポリシーに関連するアカウントに対しては、インベントリ プルのみが実行されます。

テナントの下で読み取り専用アカウントとしてアカウントを設定する場合、そのテナントのすべてのクラウドコンテキストプロファイルは読み取り専用である必要があります。そのテナントでは、通常のグリーンフィールド (Cisco Cloud APIC が作成) クラウドコンテキストプロファイルを使用できません。Cisco Cloud APIC は、クラウドのこのアカウントにリソースを作成しません。また、このアカウントのイベントまたは統計に関連する項目はクラウドに表示されません。

このアカウントはクラウド上で読み取り専用アクセス権を持ちますが、アクセスタイプは信頼できるテナントまたは信頼できないテナントのいずれかにすることができます。

## GUIを使用した読み取り専用のアカウントの設定

### 始める前に

読み取り専用のアカウントを作成する前に、[読み取り専用アカウントの概要 \(9 ページ\)](#) に示された情報をレビューします。

### 手順

---

**ステップ 1** 左のナビゲーションバーで、[アプリケーション管理 (Application Management)] > [テナント (Tenants)] に移動します。

設定済みのテナントが [テナント (Tenants)] ページに表示されます。

**ステップ 2** [アクション (Actions)] をクリックし、[テナントの作成 (Create Tenant)] を選択します。  
[テナントの作成 (Create Tenant)] ダイアログ ボックスが表示されます。

**ステップ 3** このテナントのために必要な予備情報を入力します。

[名前 (Name)]、[説明 (Description)]、および [セキュリティ ドメイン (Security Domains)] フィールドに必要な情報を入力します。

**ステップ 4** このユーザー テナントが信頼できるかどうかを決定します。

- Cloud APIC のユーザ テナントが信頼されている場合 (CFT を使用して信頼できるテナントの AWS アカウントを設定した場合は、このページに次の情報を入力します。

- [AWS アカウント ID (AWS Account ID):] ユーザ テナントの AWS アカウント番号 (CFT を使用して、信頼できるテナントの AWS アカウントをセットアップしたときにログインした AWS アカウント) を入力します。
- [アクセスタイプ (Access Type)] : このフィールドで [信頼 (Trusted)] を選択します。

(注) [クラウド アクセス キー ID (Cloud Access KEY ID)] フィールドと [クラウド秘密アクセス キー (Cloud Secret Access Key)] フィールドは、[アクセスタイプ (Access Type)] として [信頼済み (Trusted)] を選択している場合、表示されません。これらのフィールドは、信頼できるテナントには必要ありません。

- Cloud APIC のユーザ テナントが信頼されていない場合 (AWS アクセスキー ID と秘密アクセス キーを使用して、信頼できないユーザ テナントの AWS アカウントをセットアップした場合は、このページで次の情報を入力します。

- [AWS アカウント ID (AWS Account ID):] このフィールドには、ユーザ テナントの AWS アカウント番号を入力します。
- Access Type : このフィールドで [Untrusted] を選択します。

- **[クラウドアクセス キー ID (Cloud Access KEY ID):]** このフィールドには、ユーザテナントの AWS アクセスキー ID 情報を入力します。
  - **[クラウド秘密アクセス キー (Cloud Secret Access Key):]** このフィールドには、ユーザテナントの AWS 秘密アクセス キー情報を入力します。
- ユーザテナントがAWS組織のメンバーである場合（AWS組織を使用して組織を設定し、組織内にアカウントを作成するか、組織にアカウントを招待することでアカウントを追加した場合）、組織のマスターアカウントの場合は、次の情報を入力して組織タグをこのテナントに割り当てます。 Cloud APIC
- **[AWS アカウント ID (AWS Account ID):]** このフィールドには、ユーザテナントの AWS アカウント番号を入力します。
  - **[アクセスタイプ (Access Type) ]:** このフィールドで**[組織 (Organization) ]**を選択します。
    - (注) このテナントに組織タグを割り当てる場合は、以下が適用されます。
      - このフィールドで**[組織 (Organization) ]**オプションがグレー表示されている場合は、AWS組織のマスターアカウント（インフラストラクチャテナント）を展開していません。 Cloud APIC（インフラテナント）がAWS組織のマスターアカウントに展開されていない場合、テナントに組織タグを割り当てることはできません。 Cloud APIC
      - 既存の AWS アカウントに招待されたマスターアカウントが組織に加わる場合、組織テナント用のAWSに設定された OrganizationAccountAccessRole IAM ロールがあり、Cloud APIC 関連の許可を使用可能であることを確認してください。
- (注) **[クラウドアクセス キー ID (Cloud Access KEY ID)]** フィールドと **[クラウド秘密アクセス キー (Cloud Secret Access Key)]** フィールドは、**[アクセス タイプ (Access Type) ]**として**[信頼済み (Trusted) ]**を選択している場合、表示されません。これらのフィールドは、組織テナントには必要ありません。

**ステップ 5** **[クラウドアクセス権限 (Cloud Access Privilege) ]**フィールドで、**[読み取り専用 (Read Only) ]**を選択します。

このフィールドは、クラウドアカウントを読み取り専用を設定します。この AWS アカウントにはブラウнフィールド VPC（アンマネージドのリソース）のみを持つことができます。

このフィールドで **[読み取りと書き込み (Read and Write) ]** オプションをクリックした場合、これは、このテナントがグリーンフィールドとブラウнフィールドの両方の VPC（マネージドリソースとアンマネージドリソース両方）を持つことができることを意味し、[読み取り専用アカウントの概要（9 ページ）](#)に記載されている読み取り専用アカウントにする場合は、望む結果とは異なります。

**ステップ 6** このテナントの残りの設定を完了し、完了したら **[保存 (Save) ]** をクリックします。

## 次のタスク

[管理対象外（ブラウフィールド）クラウド コンテキスト プロファイルの作成（12 ページ）](#) で提供される情報を使用したアンマネージド（ブラウフィールド）クラウド コンテキスト プロファイルの作成

## REST API を使用した読み取り専用アカウントの設定

### 始める前に

読み取り専用のアカウントを作成する前に、[読み取り専用アカウントの概要（9 ページ）](#) に示された情報をレビューします。

### 手順

クライアント シークレットを使用して読み取り専用アカウントでアンマネージドテナントを作成するには、以下を投稿します。

太字のテキストは、クラウド アカウントを読み取り専用を設定する行を示しています。

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="unmanagedTenant1">
  <cloudAwsProvider accountId="976500909689"
    accessKeyId="XXXXXXXXXXXXXXXXXXXX"
    secretAccessKey="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
    providerId="aws">
    <cloudRsProviderToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only"/>
  </cloudAwsProvider>
</fvTenant>
```

## 次のタスク

[管理対象外（ブラウフィールド）クラウド コンテキスト プロファイルの作成（12 ページ）](#) で提供される情報を使用したアンマネージド（ブラウフィールド）クラウド コンテキスト プロファイルの作成

## 管理対象外（ブラウフィールド）クラウド コンテキスト プロファイルの作成

次のトピックでは、アンマネージド（ブラウフィールド）クラウド コンテキスト プロファイルを作成する方法について説明します。

## アンマネージド（ブラウフィールド）クラウド コンテキスト プロファイルの概要

アンマネージド（ブラウフィールド）クラウド コンテキスト プロファイルは、アンマネージド（ブラウフィールド）VPC に関連付けられている Cisco Cloud APIC ポストされた構成を参照します。

アカウントは、読み取り / 書き込みアクセス（グリーンフィールド VPC とブラウフィールド VPC の両方の作成をサポートできます）または読み取り専用アクセス（ブラウフィールド VPC の作成のみをサポートできます）を持つことができます。したがって、デフォルトのアクセス ポリシー（読み取り/書き込み）を持つアカウントの下と、読み取り専

用アクセスポリシーを持つアカウントの下に、アンマネージド(ブラウンフィールド)クラウドコンテキストプロファイルを作成できます。

さらに、すでにCisco Cloud APIC構成済みのVPCがあり、同じAWSアカウント内にアンマネージドVPCも存在する、デフォルトのアクセスポリシー(読み取り/書き込み)のアカウントを有している場合、このアカウントに関連付けられたテナントでアンマネージドクラウドコンテキストプロファイルを定義できます。つまり、グリーンフィールドクラウドコンテキストプロファイルで使用されているテナントがすでに作成されている場合、その同じテナントをブラウンフィールドクラウドコンテキストプロファイル(アンマネージドVPCのインポート)の作成にも使用できます。

アンマネージド(ブラウンフィールド)クラウドコンテキストプロファイルに設定する必要があるパラメータは次のとおりです。

- **VRF** : アンマネージドVPCを関連付けるCisco Cloud APICのVRF
- **リージョン** : アンマネージドVPCがクラウド上に存在するリージョン
- **VNet ID** : クラウド上のこのアンマネージドVPCのクラウドプロバイダーID
- **CIDR** : Cisco Cloud APICで参照する必要があるCIDR

Cisco Cloud APICはこれらのパラメータを使用して、ブラウンフィールドクラウドコンテキストプロファイルをクラウド上の特定のVPCにマッピングします。

## GUIを使用したアンマネージド(ブラウンフィールド)クラウドコンテキストプロファイルの作成

### 始める前に

これらの手順を実行する前に、[アンマネージド\(ブラウンフィールド\)クラウドコンテキストプロファイルの概要\(12ページ\)](#)に記載されている情報を確認してください。

### 手順

---

**ステップ 1** 必要な場合は、アンマネージド(ブラウンフィールド)クラウドコンテキストプロファイルで使用する新しいテナントを作成します。

アンマネージド(ブラウンフィールド)VPCが別のAWSにある場合、新しいテナントを作成する必要があります。

新しいテナントを作成する手順については、『[Cisco Cloud APIC for AWS User Guide](#)』、リリース25.0(x)以降の「リリース4.2(3)およびそれ以降向けテナントAWSの構成」を参照してください。

このテナントは、AWS内のアンマネージド(ブラウンフィールド)VPCと同じAWSアカウントを使用する必要があります。

**ステップ 2** ブラウンフィールドVPCのクラウドコンテキストプロファイルに関連付けるVRFを作成します。

- a) Cisco Cloud APIC GUIの左側のナビゲーションバーで、**[Application Management] > [VRF]** をクリックします。

設定されている VRF リストが表示されます。

- b) [アクション (Actions) ] > [VRF の作成 (Create VRF) ] をクリックします。

[VRF の作成 (Create VRF) ] ページが表示されます。

- c) 次の [VRF ダイアログボックスの作成 (Create VRF) ] ダイアログボックスのフィールドの表に示されているように、各フィールドに適切な値を入力し、続行します。

表 1: [VRF の作成 (Create VRF) ] ダイアログボックスのフィールド

[プロパティ (Properties) ]	説明
全般	
名前	[Name] フィールドに、VRF の表示名を入力します。 すべての VRF に <i>vrfEncoded</i> 値が割り当てられます。テナントと VRF 名の組み合わせが 32 文字を超える場合、VRF 名 (テナント名も含む) は <i>vrfEncoded</i> 値を使用してクラウドルータで識別されます。 <i>vrfEncoded</i> 値を表示するには、[Application Management] > [VRFs] サブタブに移動します。右側のペインで VRF をクリックし、クラウドルータで [Encoded VRF Name] を探します。
テナント	テナントを選択します。 <b>1.</b> [テナントの選択 (Select Tenant) ] をクリックします。[テナントの選択 (Select Tenant) ] ダイアログボックスが表示されます。 <b>2.</b> [テナントの選択 (Select Tenant) ] ダイアログで、左側の列のテナントをクリックして選択し、アンマネージド (ブラウンフィールド) VPC に関連付けられているテナントを選択します。 <b>3.</b> [選択 (Select) ] をクリックします。 [VRF の作成 (Create VRF) ] ダイアログボックスに戻ります。
説明	VRF の説明を入力します。

- d) 作業が完了したら、[保存 (Save) ] をクリックします。

**ステップ 3** Cisco Cloud APIC GUI で、[Intent] アイコン (🔗) をクリックします。

ウィンドウの右側に、何をしますかを尋ねるスライドイン ペインが表示されます。

**ステップ 4** [アンマネージド VPC (Unmanaged VPC) ] オプションをクリックします。

アンマネージドクラウド コンテキスト プロファイルを作成するためのセットアップ ウィザードが表示されます。

**ステップ 5** [アンマネージド VPC の関連付け (Unmanaged VPC Association)] ウィンドウの [設定 (Settings)] 領域で、[アンマネージド VPC (Unmanaged VPC)] フィールドの下の [アンマネージド VPC の選択 (Select Unmanaged VPC)] をクリックします。

[アンマネージド VPC の選択 (Select Unmanaged VPC)] ウィンドウが表示され、テナントを作成した AWS アカウントで AWS で使用可能なすべてのブラウフィールド VPC (Cisco Cloud APIC によって管理されていない VPC) が表示されます。このウィンドウに入力される VPC のリストは、この AWS アカウントのインベントリ プルに基づいています。

(注) インベントリ プルが完了するまでに 8 ~ 10 分かかる場合があるため、ブラウフィールド VPC がリストされていない場合は、インベントリ プルが完了するまで 8 ~ 10 分待ちます。

**ステップ 6** インポートするアンマネージド VPC をリストから探し、アンマネージドクラウドコンテキストプロファイルに関連付けます。

Cisco Cloud APIC GUI のこのウィンドウでは、このリストのアンマネージド VPC が [クラウドプロバイダー ID (Cloud Provider ID)] 列の形式で表示されます。

**VPC\_ID**

**AWS > {tenant} > {AWS\_region}**

Cisco Cloud APIC GUI ページの [名前 (Name)] 列のブラウフィールド VPC の名前。

<https://console.aws.amazon.com/vpc/>にある Amazon VPC コンソールに移動し、AWS ページで管理されていない VPC を特定し、このブラウフィールド VPC の [名前 (Name)] および [VPC ID] フィールドを特定して、情報が GUI ページに表示される情報と一致していることを確認します。

<https://console.aws.amazon.com/vpc/> Cisco Cloud APIC

**ステップ 7** リストから適切なアンマネージド VPC をクリックします。

ウィンドウの右側のペインに、このアンマネージド VPC に関する追加情報が表示されます。

**ステップ 8** [選択 (Select)] をクリックします。

[アンマネージド VPC 関連付けのインポート (Import Unmanaged VPC Association)] のメインウィンドウに戻ります。

**ステップ 9** [テナント (Tenant)] フィールドに、テナント エントリが自動的に入力されます。

リストからインポートするアンマネージド VPC を選択すると、対応するテナントがこのフィールドに自動的に入力されます。このアンマネージドクラウドコンテキストプロファイルは、このテナントの下に作成されます。

**ステップ 10** [VRF] フィールドで、このアンマネージドクラウドコンテキストプロファイルに関連付ける VRF を選択します。

**ステップ 11** [クラウドコンテキスト プロファイルの名前 (Cloud Context Profile Name)] フィールドに、プロファイルの名前を入力します。

**ステップ 12** [TGW アタッチメント (TGW Attachment)] フィールドで、[Enable] の横にあるボックスをクリックして、このアンマネージドクラウドコンテキストプロファイルの AWS トランジットゲートウェイを有効にします。

このフィールドを有効にすると、次の手順でハブネットワークとトランジットゲートウェイルートテーブルの関連付けスコープを選択できます。これらのステップで行った選択に基づいて、ルートテーブルがインフラ トランジット ゲートウェイに作成されます。詳細については、ドキュメント「AWS トランジット ゲートウェイまたは AWS トランジット ゲートウェイ コネクトを使用した VPC 間の帯域幅の増加」を参照してください。

**ステップ 13** [ハブ ネットワーク (Hub Network)] フィールドで、このクラウド コンテキスト プロファイルに関連付けるハブ ネットワークを選択します。

AWS トランジット ゲートウェイまたは AWS トランジット ゲートウェイ コネクトを最初にセットアップしたときに、このハブ ネットワークを作成しておく必要があります。ハブ ネットワークをまだ作成していない場合は、ドキュメント「AWS トランジット ゲートウェイまたは AWS トランジット ゲートウェイ コネクトを使用した VPC 間の帯域幅の増加」に記載されている手順を使用して、ハブ ネットワークを作成します。

**ステップ 14** [TGW ルート テーブル 関連付けの範囲 (TGW Route Table Association Scope)] フィールドで、次のオプションのいずれかを選択します。

次の選択はリリース 25.0(2) 以降の変更に基づき、AWS トランジット ゲートウェイの構成時に、デフォルトでトランジットゲートウェイルートテーブルが VRF ごとに展開されます。この変更の一環として、トランジットゲートウェイルートテーブルのラベルベースの展開も利用可能になり、新しいラベルごとに、そのラベルにちなんで名付けられた新しいトランジットゲートウェイルートテーブルが展開されます。詳細については、ドキュメント「AWS トランジットゲートウェイまたは AWS トランジットゲートウェイコネクトを使用した VPC 間の帯域幅の増加」の「トランジットゲートウェイ外部ネットワーク」の項を参照してください。 <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/cloud-apic/5-x/use-case/increasing-bandwidth-using-aws-transit-gateway-or-aws-transit-gateway-connect.html>

- ネットワーク レベル：ネットワークまたは VRF レベルでトランジットゲートウェイルートテーブルを展開する場合は、このオプションを選択します。

[TGW ルート テーブル関連付けラベル (TGW Route Table Association Label)] フィールドでは、トランジットゲートウェイルートテーブルの名前が次の形式を使用して自動的に入力されます。

```
<tenantName>-<vrfName>
```

- アカウント レベル：アカウントまたはテナント レベルでトランジットゲートウェイルートテーブルを展開する場合は、このオプションを選択します。

[TGW ルート テーブル関連付けラベル (TGW Route Table Association Label)] フィールドでは、トランジットゲートウェイルートテーブルの名前が次の形式を使用して自動的に入力されます。

```
<tenantName>
```

- ラベル ベース：トランジットゲートウェイルートテーブルの展開にカスタムラベルを使用する場合は、このオプションを選択します。VPC は、このカスタムラベルに基づいて展開されたトランジットゲートウェイルートテーブルに関連付けられます。

[カスタムラベル (Custom Label)] 領域で [カスタムラベルの選択 (Select Custom Label)] をクリックし、トランジットゲートウェイルートテーブルの展開に使用するカスタムラベルを選択します。

**ステップ 15** [インポートするリソース (**Resources to Import**)] 領域で、必要に応じて、このアンマネージドクラウドコンテキストプロファイルにインポートするアンマネージド VPC 内で使用可能な追加の CIDR を選択します。

- アンマネージド VPC のプライマリ CIDR ブロック範囲は自動的にインポートされ、プライマリ CIDR としてタグ付けされます。
- [CIDR の追加 (Add CIDR)] をクリックして、アンマネージド VPC 内に CIDR を追加します。この領域にリストされているすべての CIDR を選択するか、このアンマネージドクラウドコンテキストプロファイルにインポートする特定の CIDR を選択できます。

[インポートするリソース (**Resources to Import**)] 領域に表示されるすべての CIDR について、対応するサブネットもインポートされます。

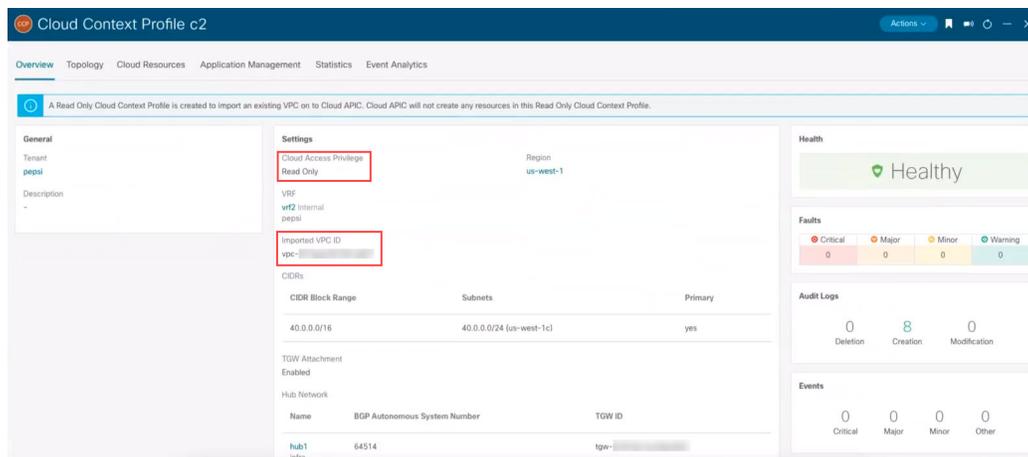
**ステップ 16** [アンマネージド VPC 関連付けのインポート (Import Unmanaged VPC Association)] ウィンドウで [保存 (Save)] をクリックして、このクラウドコンテキストプロファイルを保存します。

[What's Next] ページが表示されます。

**ステップ 17** ウィンドウの右下にある [クラウドコンテキストプロファイルの詳細に移動 (Go to Cloud Context Profile Details)] をクリックします。

先ほど作成したクラウドコンテキストプロファイルの詳細画面が表示されます。

次の図は、読み取り専用フラグが有効になっており、関連付けられている VPC ID が設定されたアンマネージドクラウドコンテキストプロファイルを示しています。



**ステップ 18** Cisco Cloud APIC GUI の左側のナビゲーションバーで、[Application Management] > [VRF] をクリックします。

設定されている VRF リストが表示されます。

**ステップ 19** ブラウンフィールド VPC のクラウドコンテキストプロファイルに関連付けられるこれらの手順で以前に作成した VRF を特定し、その VRF をクリックします。

VRF がインポートされたブラウンフィールド VPC に関連付けられていることを確認します。

---

## 次のタスク

[AWS でのアンマネージド VPC のトランジット ゲートウェイ アタッチメントの追加 \(19 ページ\)](#) で提供されている手順を使用して、アンマネージド (ブラウフィールド) VPC と AWS のインフラ トランジット ゲートウェイの間に AWS トランジット ゲートウェイ アタッチメントを構成します。

## REST API を使用したアンマネージド (ブラウフィールド) クラウド コンテキスト プロファイルの作成

### 始める前に

これらの手順を実行する前に、[アンマネージド \(ブラウフィールド\) クラウド コンテキスト プロファイルの概要 \(12 ページ\)](#) に記載されている情報を確認してください。

### 手順

アンマネージド (ブラウフィールド) のクラウド コンテキスト プロファイルを作成するには、以下を投稿します。

以下のエリアでは、アンマネージド クラウド コンテキスト プロファイルの作成に使用される行を示しています。

- `cloudRsCtxProfileToAccessPolicy` 行は、クラウド コンテキスト プロファイルを読み取り専用を設定します (詳細については、[読み取り専用アカウントの概要 \(9 ページ\)](#) を参照してください)。
- `cloudBrownfield` および `cloudIDMapping` 行は、AWS クラウドのブラウフィールド VPC の VPC ID を使用して、ブラウフィールド VPC をインポートするために使用されます。
- `cloudRsCtxProfileToRegion` 行は、VPC が AWS クラウドに存在するリージョンを指します。
- `cloudCidr` の行は、AWS クラウドの CIDR と一致する 1 つ以上の CIDR (そのうちの 1 つがプライマリ CIDR) です。

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml
<fvTenant name="unmanagedTenant1">
  <fvCtx name="vrf1" />
    <cloudCtxProfile name="BrownfieldCtxProfile1">
      <cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only"/>
      <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-west-1"/>
      <cloudRsToCtx tnFvCtxName="vrf1" />
      <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default-foo"
label="system='vrf'"/>
      <cloudBrownfield status="">
      <cloudIDMapping cloudProviderId="vpc-0fe1afe17568417c8"/>
    </cloudBrownfield>
      <cloudCidr name="cidr1" addr="40.0.0.0/16" primary="yes" />
    </cloudCtxProfile>
  </fvTenant>
```

## 次のタスク

ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成 (20 ページ) に示す情報を使用して、ブラウフィールドクラウドコンテキストプロファイルに関連付ける EPG を作成します。

# AWS でのアンマネージド VPC のトランジットゲートウェイアタッチメントの追加

このタスクでは、アンマネージド (ブラウフィールド) VPC のトランジットゲートウェイアタッチメントについて (5 ページ) で説明されているように、アンマネージド (ブラウフィールド) VPC と AWS のインフラトランジットゲートウェイ間に AWS トランジットゲートウェイアタッチメントを構成します。

ブラウフィールド VPC ができることとできないこと Cisco Cloud APIC (6 ページ) および アンマネージド (ブラウフィールド) VPC のトランジットゲートウェイアタッチメントについて (5 ページ) で説明されているように、Cisco Cloud APIC はアンマネージド (ブラウフィールド) VPC と AWS のインフラトランジットゲートウェイ間の AWS トランジットゲートウェイアタッチメントを構成しません。インフラ構成の一部として Cisco Cloud APIC によって作成された AWS トランジットゲートウェイは、ブラウフィールド AWS ユーザーアカウントと共有されますが、Cisco Cloud APIC にインポートしたブラウフィールド VPC のすべての共有インフラトランジットゲートウェイを使用して、トランジットゲートウェイ VPC アタッチメントを手動で作成する必要があります。

## 始める前に

これらの手順を開始する前に、管理対象外 (ブラウフィールド) クラウドコンテキストプロファイルの作成 (12 ページ) の手順を実行してください。これらの手順の最後に、Cisco Cloud APIC はすべてのインフラトランジットゲートウェイを使用してトランジットゲートウェイ VPC アタッチメントを構成します。

## 手順

---

**ステップ 1** AWS ポータルで、[トランジットゲートウェイアタッチメント (Transit Gateway Attachments)] に移動します。

[トランジットゲートウェイアタッチメント (Transit Gateway Attachments)] ページが表示されます。

**ステップ 2** [トランジットゲートウェイアタッチメントの作成 (Create transit gateway attachment)] をクリックします。

[トランジットゲートウェイアタッチメントの作成 (Create transit gateway attachment)] ページが表示されます。

**ステップ 3** [詳細 (Details)] 領域で、作成するトランジットゲートウェイアタッチメントに必要な情報を入力します。

- [名前タグ (Name tag)] フィールドに、このトランジットゲートウェイアタッチメントの名前タグを入力します。

- [トランジットゲートウェイ ID (Transit gateway ID)] フィールドで、ブラウフィールドユーザーアカウントと共有されたグリーンフィールド VPC 構成の一部として作成された AWS トランジットゲートウェイを選択します。
- [アタッチメントタイプ (Attachment type)] フィールドで、[VPC] を選択します。

ステップ 4 [VPC アタッチメント (VPC Attachment)] エリアで、作成するトランジットゲートウェイアタッチメントに必要な情報を入力します。

- [DNS サポート (DNS support)] フィールドは選択したままにし、[IPv6 サポート (IPv6 support)] フィールドは選択しないでください。
- [VPC ID] フィールドで、ブラウフィールド VPC ID を選択します。

ステップ 5 残りのフィールドのデフォルト エントリはそのままにして、[トランジットゲートウェイアタッチメントの作成 (Create transit gateway attachment)] をクリックします。

---

## 次のタスク

[ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成 \(20 ページ\)](#) に示す情報を使用して、ブラウフィールドクラウドコンテキストプロファイルに関連付ける EPG を作成します。

# ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成

次のトピックでは、ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG の作成について説明します。

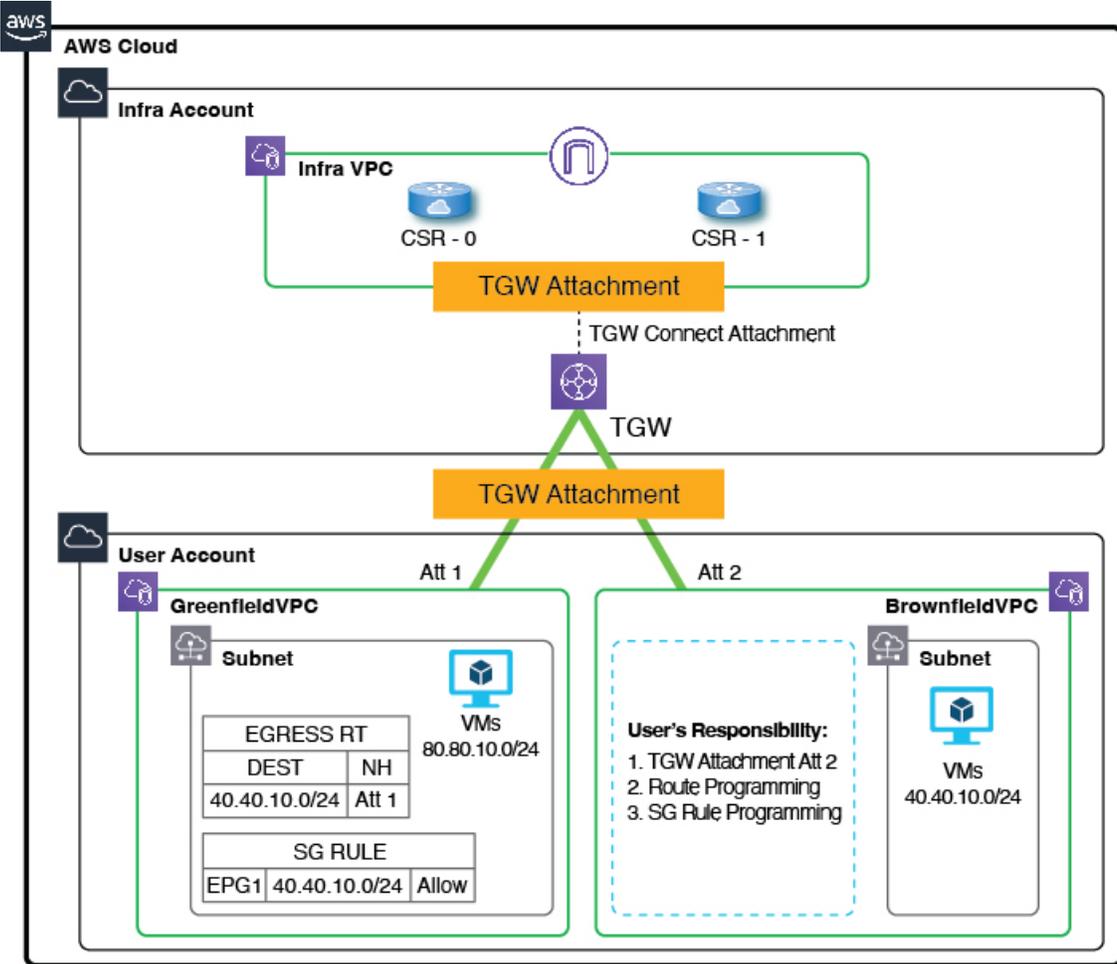
## EPG が VRF を通じたブラウフィールドクラウドコンテキストプロファイルと関連付けられている方法

EPG が VRF を介してブラウフィールドクラウドコンテキストプロファイルに関連付けられていることをよりよく理解するために、EPG が正常にマッピングされる方法と比較すると役立ちます。

- **通常の EPG マッピング** : 通常、通常のクラウド EPG を定義する場合は、クラウド EPG を VRF に関連付けます。クラウドコンテキストプロファイルも、このプロセスの一部として VRF に関連付けられます。したがって、EPG が定義されると、EPG はこの VRF に関連付けられたすべてのクラウドコンテキストプロファイル (VPC) の下の適切なセキュリティグループに変換され、AWS クラウドでセキュリティグループルールに変換されます。
- **ブラウフィールドクラウドコンテキストプロファイルに関連付けられている EPG** : アンマネージド (ブラウフィールド) クラウドコンテキストプロファイルが定義され、VRF に関連付けられている場合、およびこの同じ VRF に関連付けられている EPG を定義すると、この EPG は **ブラウフィールドクラウドコンテキストプロファイルと関連付けられた EPG** と呼ばれます。ブラウフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成する理由は、グリーンフィールド VPC 上のセキュリティやルーティングなど、Cisco Cloud APIC

のすべてのネットワーキングおよびセキュリティ構造をオーケストレーションして、ブラウンフィールド VPC への通信を可能にするためです。

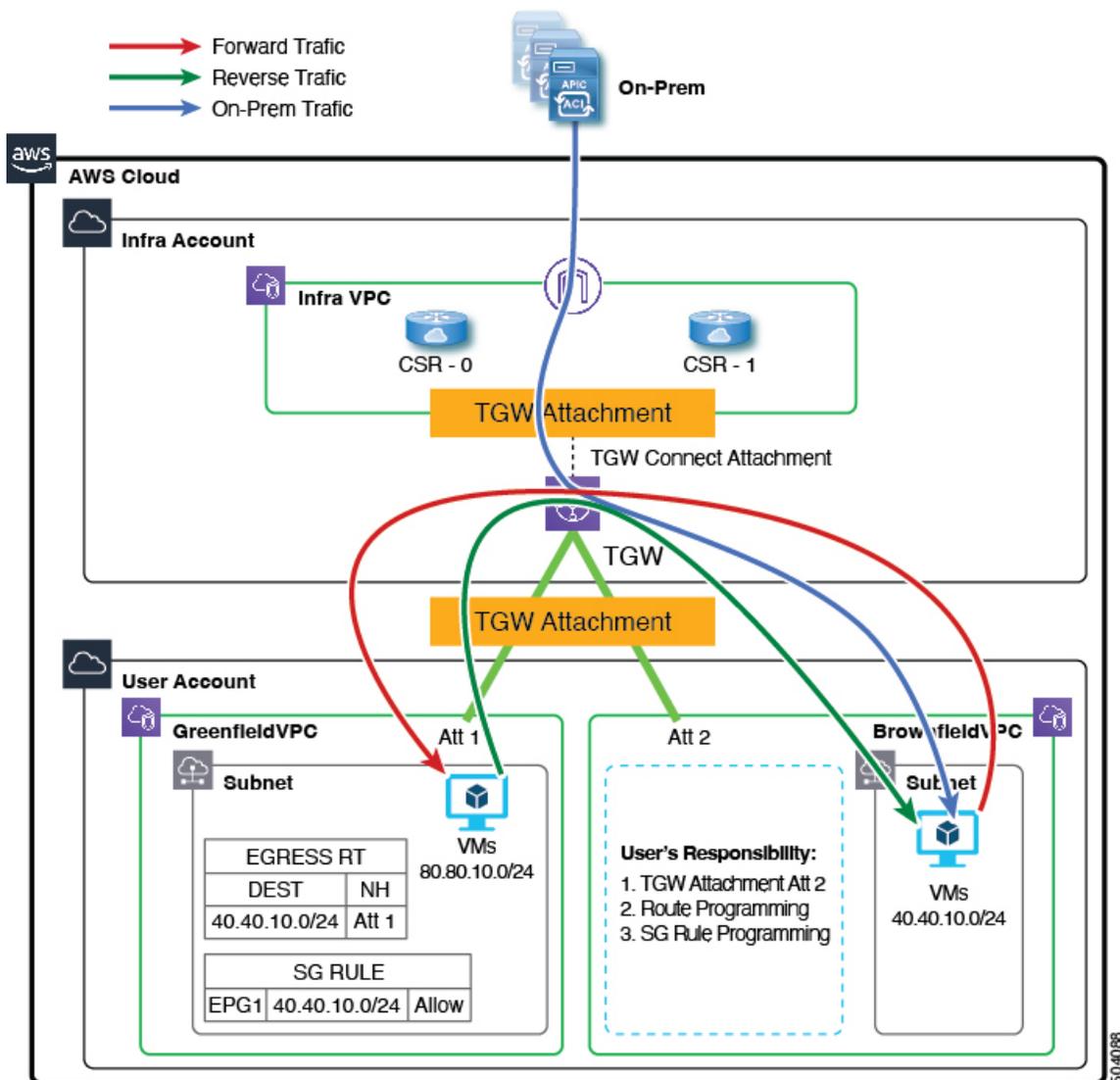
たとえば、次の図の設定を考えます。



この設定では、ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられた EPG を作成し、契約を作成する理由は、グリーンフィールド VPC 側のルーティングとセキュリティをプロビジョニングして、トラフィックがこのアンマネージド (ブラウンフィールド) VPC に到達できるようにするためです。

- ルートテーブルエントリとセキュリティグループルールのプログラミング、およびグリーンフィールド VPC (例の図の Att 1) のトランジット ゲートウェイ アタッチメントの作成は、すべて Cisco Cloud APIC によって行われます。
- ただし、**ブラウンフィールド VPC** の場合、Cisco Cloud APIC はルートテーブルエントリとセキュリティグループルールをプログラムせず、Cisco Cloud APIC はブラウンフィールド VPC のトランジット ゲートウェイ アタッチメントを作成しません。したがって、ブラウンフィールド VPC に対してこれらの構成を手動で行う必要があります。
- Cisco Cloud APIC グリーンフィールド VPC とブラウンフィールド VPC 間のルーティングを許可するように CSR をプログラムします。

この例の目標は、グリーンフィールド VPC のパケットフローが 40.40.10.0/24 (セキュリティ グループルール) にパケットを送受信できるようにし、このサブネット宛てのトラフィックをインフラ トランジット ゲートウェイに送信して、CSR をブラウンフィールド VPC にパケットを送信します。これらはすべてコントラクトを使用して実現されます。



Cisco Cloud APIC は、ブラウンフィールド VPC 側のルート エントリまたはセキュリティグループルールをプログラムしません。代わりに、Cisco Cloud APIC はコントラクトに基づいてブラウンフィールド VPC サブネットとの間でパケットを送受信するようにグリーンフィールド VPC 側のみをプログラムします。Cisco Cloud APIC は、グリーンフィールド VPC とブラウンフィールド VPC の間でルーティングが発生するように CSR を適宜プログラムします。

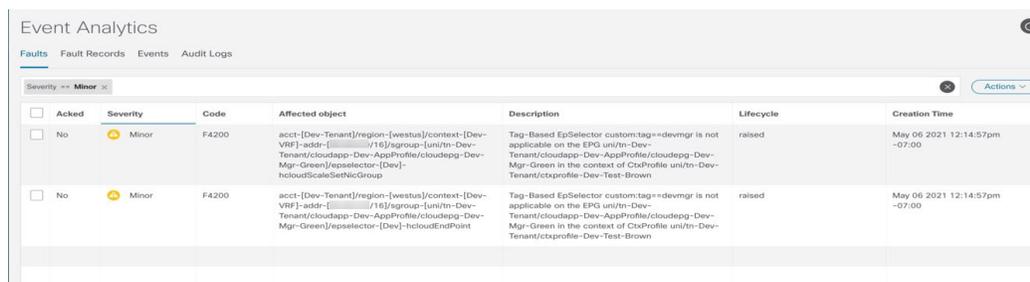
そのため、ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられた EPG を作成し、他のグリーンフィールド VPC がブラウンフィールド VPC との間でトラフィックを送受信できるようにします。

ブラウンフィールドクラウド コンテキスト プロファイルに関連付けられている EPG には、サブネットベースまたは正確な IP ベースのエンドポイントセレクタのみがあり、タグベースのエンドポイントセレクタはないことに注意して

ください。Cisco Cloud APIC はアンマネージド VPC に属するエンドポイントを認識しません。このため、Cisco Cloud APIC はアンマネージド（ブラウンフィールド）の VPC に属するタグベースのエンドポイントを認識しません。Cisco Cloud APIC がエンドポイントを検出できない場合、IP アドレスが見つからないため、グリーンフィールド VPC 側のセキュリティルールをプログラムして、ブラウンフィールド VPC 側との間でパケットを送受信することはできません。

ブラウンフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成し、その EPG でサブネットベースまたは特定の IP ベースのエンドポイントセレクタを定義する理由は次のとおりです。

- この EPG（ブラウンフィールドクラウドコンテキストプロファイルに関連付けられている）から別の EPG（グリーンフィールドクラウドコンテキストプロファイルに関連付けられている）へのコントラクトを作成すると、グリーンフィールド VPC 側のルートテーブルにあるアンマネージド VPC CIDR へのルートエントリのプログラミングが実行されます。
- これにより、グリーンフィールド VPC 側のすべてのセキュリティグループルールがプログラミングされ、EPG のエンドポイントセレクタで定義されたこれらのサブネットとの間でパケットを送受信できるようになります。
- EPG がタグベースのエンドポイントセレクタで設定され、ブラウンフィールドクラウドコンテキストプロファイルに関連付けられている場合は、この EPG を使用できないというエラーが発生します。



Acked	Severity	Code	Affected object	Description	Lifecycle	Creation Time
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VRF]-addr-[redacted]/16/ragroup-[uni/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudScaleSetNicGroup	Tag-Based EpSelector custom:tag=devmgr is not applicable on the EPG uni/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile uni/n-Dev-Tenant/ctxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00
<input type="checkbox"/>	Minor	F4200	acct-[Dev-Tenant]/region-[westus]/context-[Dev-VRF]-addr-[redacted]/16/ragroup-[uni/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green]/epselector-[Dev]-hcloudEndPoint	Tag-Based EpSelector custom:tag=devmgr is not applicable on the EPG uni/n-Dev-Tenant/cloudapp-Dev-AppProfile/cloudapp-Dev-Mgr-Green in the context of CtxProfile uni/n-Dev-Tenant/ctxprofile-Dev-Test-Brown	raised	May 06 2021 12:14:57pm -07:00

## GUI を使用したブラウンフィールドクラウドコンテキストプロファイルと関連付けられた EPG の作成

このトピックでは、ブラウンフィールドクラウドコンテキストプロファイルに関連付けられた EPG を作成します。これを行う必要がある理由については、[EPG が VRF を通じたブラウンフィールドクラウドコンテキストプロファイルと関連付けられている方法（20 ページ）](#) を参照してください。

### 始める前に

次の手順を実行する前に、次の手順を実行する前に、必要なすべての設定が完了していることを確認します。

- [GUI を使用したアンマネージド（ブラウンフィールド）クラウドコンテキストプロファイルの作成（13 ページ）](#)

### 手順

**ステップ 1** インテントアイコンをクリックします。

[**インテント (Intent)**] メニューが表示されます。

ステップ2 [インテント (Intent)] 検索ボックスの下にあるドロップダウン矢印をクリックし、[アプリケーション管理 (Application Management)] を選択します。

[アプリケーション管理 (Application Management)] オプションのリストが[インテント (Intent)] メニューに表示されます。

ステップ3 [インテント (Intent)] メニューの[アプリケーション管理 (Application Management)] リストで、[EPGの作成 (Create EPG)] をクリックします。

[EPGの作成 (Create EPG)] ダイアログボックスが表示されます。

ステップ4 EPGに必要な一般設定を入力します。

表 2: [EPGの作成 (Create EPG)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
全般	
名前	ブラウフィールドクラウド コンテキスト プロファイルに関連付けられた EPG の名前を入力します。
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> <li>[テナントの選択 (Select Tenant)] をクリックします。[テナントの選択 (Select Tenant)] ダイアログボックスが表示されます。</li> <li>[テナントの選択 (Select Tenant)] ダイアログで、左側の列のテナントをクリックして選択します。 アンマネージド (ブラウフィールド) VPC に関連付けられているテナントを選択します。</li> <li>[選択 (Select)] をクリックします。[EPGの作成 (Create EPG)] ダイアログボックスに戻ります。</li> </ol>
アプリケーションプロファイル	<p>アプリケーションプロファイルを選択します。</p> <ol style="list-style-type: none"> <li>[アプリケーションプロファイルの選択 (Select Application Profile)] をクリックします。[アプリケーションプロファイルの選択 (Select Application Profile)] ダイアログボックスが表示されます。</li> <li>[アプリケーションプロファイルの選択 (Select Application Profile)] ダイアログで、左側の列のアプリケーションプロファイルをクリックして選択します。</li> <li>[選択 (Select)] をクリックします。[EPGの作成 (Create EPG)] ダイアログボックスに戻ります。</li> </ol>
説明	EPG の説明を入力します。
[設定 (Settings)]	

[プロパティ (Properties) ]	説明
タイプ (Type)	EPG タイプとして [アプリケーション (Application) ] を選択します。
VRF	<p>VRF を選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. [VRF の選択 (Select VRF) ] をクリックします。[VRF の選択 (Select VRF) ] ダイアログボックスが表示されます。</li> <li>2. [VRF の選択 (Select VRF) ] ダイアログで、左側の列の VRF をクリックして選択します。ブラウフィールドクラウド コンテキスト プロファイルに関連付けられている VRF を選択します。</li> <li>3. [選択 (Select) ] をクリックします。[EPG の作成 (Create EPG) ] ダイアログボックスに戻ります。</li> </ol>
ルート到達可能性	ルートの到達可能性に対して選択されたデフォルトの [インターネット (Internet) ] オプションをそのままにします。
エンドポイントセクタ	<p>AWS ブラウフィールド サイトに対応するサブネットベースまたは特定の IP ベースのエンドポイントセクタを定義します。</p> <p>詳細については、「<a href="#">EPG が VRF を通じたブラウフィールドクラウドコンテキストプロファイルと関連付けられている方法 (20 ページ)</a>」を参照してください。</p> <ol style="list-style-type: none"> <li>1. [エンドポイントセクタの追加 (Add Endpoint Selector) ] をクリックして、エンドポイントセクタを追加します。</li> <li>2. [名前 (Name) ] フィールドに名前を入力します。</li> <li>3. [一致表現 (Match Expressions) ] 領域に次の情報を入力します。 <ul style="list-style-type: none"> <li>• キー: <b>IP</b> を選択します。</li> <li>演算子: <b>equals (==)</b> を選択します。</li> <li>• 値: 適切なサブネットベースまたは特定の IP ベースの IP エンドポイントを入力します。</li> </ul> <p>たとえば、これは、Cloud APIC にインポートするブラウフィールド VPC のリソースグループ内の仮想マシンの [プライベート IP アドレス (Private IP address) ] です。</p> </li> <li>4. この一致表現でこれらの値を受け入れるには、チェックマークをクリックします。</li> <li>5. [追加 (Add) ] をクリックして、このエンドポイントセクタを追加します。</li> <li>6. 必要に応じて、[エンドポイントセクタの追加 (Add Endpoint Selector) ] を再度クリックして、エンドポイントセクタを追加します。</li> </ol>

ステップ5 この EPG を保存するには、[保存 (Save)] をクリックします。

## 次のタスク

GUI を使用した EPG 間のコントラクトの作成 (26 ページ) に示す手順を使用して、EPG 間のコントラクトを設定します。

## GUI を使用した EPG 間のコントラクトの作成

このトピックでは、ブラウフィールドクラウド コンテキスト プロファイルに関連付けられた EPG からグリーンフィールドクラウドコンテキストプロファイルに関連付けられた外部 EPG に使用されるコントラクトを作成します。これは、グリーンフィールド VPC 側のルートテーブル内のアンマネージド VPC CIDR へのルートエントリのプログラミングを実行するために行われます。これにより、グリーンフィールド VPC 側のすべてのセキュリティグループルールがプログラミングされ、EPG のエンドポイントセレクタで定義されたこれらのサブネットとの間でパケットを送受信できるようになります。

## 始める前に

GUI を使用したブラウフィールドクラウド コンテキスト プロファイルと関連付けられた EPG の作成 (23 ページ) の手順に従って、ブラウフィールドクラウドコンテキストプロファイルに関連付けられた外部 EPG を作成します。

## 手順

- ステップ1 インテント アイコンをクリックします。[インテント (Intent)] メニューが表示されます。
- ステップ2 [インテント (Intent)] 検索ボックスの下にあるドロップダウン矢印をクリックし、[アプリケーション管理 (Application Management)] を選択します。
- [アプリケーション管理 (Application Management)] オプションのリストが [インテント (Intent)] メニューに表示されます。
- ステップ3 [インテント (Intent)] メニューの [アプリケーション管理 (Application Management)] リストで、[コントラクトの作成 (Create Contract)] をクリックします。[コントラクトの作成 (Create Contract)] ダイアログ ボックスが表示されます。
- ステップ4 次の [コントラクトダイアログ ボックス フィールドの作成 (Create Contract Dialog Box Fields)] テーブルにリストされているように、各フィールドに適切な値を入力して続行します。

表 3: [コントラクトの作成 (Create Contract)] ダイアログボックスのフィールド

[プロパティ (Properties)]	説明
名前 (Name)	契約の名前を入力します。

[プロパティ (Properties) ]	説明
テナント	<p>テナントを選択します。</p> <ol style="list-style-type: none"> <li>1. [テナントの選択 (Select Tenant) ]をクリックします。[テナントの選択 (Select Tenant) ]ダイアログボックスが表示されます。</li> <li>2. [テナントの選択 (Select Tenant) ]ダイアログで、左側の列のテナントをクリックして選択します。 アンマネージド (ブラウンフィールド) VPC に関連付けられているテナントを選択します。</li> <li>3. [選択 (Select) ]をクリックします。[コントラクトの作成 (Create Contract) ]ダイアログボックスに戻ります。</li> </ol>
説明	コントラクトの説明を入力してください。
[設定 (Settings) ]	
スコープ	<p>テナントの適切なスコープを選択します。</p> <ul style="list-style-type: none"> <li>• 1つのテナントの EPG が別のテナントの EPG と通信できるようにするには、[グローバル (Global) ]スコープを選択します。</li> <li>• 1つの VRF の EPG が別の VRF の別の EPG と通信できるようにするには、[グローバル (Global) ]または[テナント (Tenant) ]スコープを選択します。</li> </ul>
フィルタの追加	<p>フィルタを選択します。</p> <ol style="list-style-type: none"> <li>1. [フィルタの追加 (Add Filter) ]をクリックします。フィルタ行が表示され、[フィルタの選択 (Select Filter) ]オプションが表示されます。</li> <li>2. [フィルタの選択 (Select Filter) ]をクリックします。[フィルタの選択 (Select Filter) ]ダイアログボックスが表示されます。</li> <li>3. [フィルタの選択 (Select Filter) ]ダイアログで、左側の列のフィルタをクリックして選択し、[選択 (Select) ]をクリックするか、または必要に応じて[フィルタの作成 (Create Filter) ]をクリックして新しいフィルタを作成します。 フィルタの詳細については、『Cloud APIC for AWS Users Guide』を参照してください。 [コントラクトの作成 (Create Contract) ]ダイアログボックスに戻ります。</li> </ol>

ステップ 5 設定が終わったら [Save] をクリックします。

[次は (What's Next) ] ウィンドウが表示されます。

ステップ 6 ウィンドウの右下隅にある [詳細に移動 (Go to Details) ] をクリックします。

コントラクトの詳細ウィンドウが表示されます。

**ステップ 7** [アクション (Actions) ] > [EPG 通信 (EPG Communication) ] をクリックします。 >

[EPG 通信設定 (EPG Communication Configuration) ] ウィンドウが表示されます。

**ステップ 8** 左側の [コンシューマー EPG (Consumer EPGs) ] 領域で、 [コンシューマー EPG の追加 (Add Consumer EPGs) ] をクリックします。

[コンシューマー EPG の選択 (Select Consumer EPGs) ] ウィンドウが表示されます。

**ステップ 9** グリーンフィールドとブラウンフィールドクラウド コンテキスト プロファイルに関連付けられている EPG を選択し、 [選択 (Select) ] をクリックします。

次に例を示します。

- グリーンフィールド EPG 用に `epg1` を以前に作成していた場合
- の手順を使用して、ブラウンフィールド EPG の `epg2` を作成しました。 [GUI を使用したブラウンフィールドクラウド コンテキスト プロファイルと関連付けられた EPG の作成 \(23 ページ\)](#)

次に、 [コンシューマー EPG の選択 (Select Consumer EPGs) ] ウィンドウで `epg1` (グリーンフィールド EPG) と `epg2` (ブラウンフィールド EPG) の両方を選択します。

**ステップ 10** [選択 (Select) ] をクリックします。

[EPG 通信設定 (EPG Communication Configuration) ] ウィンドウに戻ります。

**ステップ 11** 右側の [プロバイダー EPG (Provider EPGs) ] 領域で、 [プロバイダー EPG の追加 (Add Provider EPGs) ] をクリックします。

[プロバイダー EPG の選択 (Select Provider EPGs) ] ウィンドウが表示されます。

**ステップ 12** 再度、グリーンフィールドとブラウンフィールドクラウド コンテキスト プロファイルに関連付けられている EPG を選択します。

コンシューマー EPG の手順で提供されている例を使用して、 [プロバイダー EPG の選択 (Select Provider EPGs) ] ウィンドウで同じ EPG (グリーンフィールド EPG `epg1` およびブラウンフィールド EPG `epg2`) を選択します。

**ステップ 13** [選択 (Select) ] をクリックします。

[EPG 通信設定 (EPG Communication Configuration) ] ウィンドウに戻ります。

**ステップ 14** [保存 (Save) ] をクリックします。

---

## 次のタスク

[AWS でのブラウンフィールド VPC の残りの構成の完了 \(29 ページ\)](#) の手順に従って、AWS の残りの設定タスクを完了します。

## REST API を使用してブラウンフィールドクラウドコンテキストプロファイルと関連付けられた EPG の作成

### 手順

ブラウンフィールド VPC のクラウド EPG を作成します。

クラウド EPG を作成して、オンプレミス サイトまたは別のクラウド サイトがこのアンマネージド ブラウンフィールド VPC とトラフィックを送受信できるようにします。

(注) これらのブラウンフィールドクラウド EPG のエンドポイントセクタは、タグベースではなく、サブネット ベースまたは IP ベースである必要があります。

```
<fvTenant name="unmanagedTenant1">
  <fvCtx name="vrf1" />
  <cloudCtxProfile name="BrownfieldCtxProfile1">
    <cloudRsCtxProfileToAccessPolicy tDn="uni/tn-infra/accesspolicy-read-only"/>
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-aws/region-us-west-1"/>
    <cloudRsToCtx tnFvCtxName="vrf1" />
    <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default-foo"
label="system=='vrf'"/>
    <cloudBrownfield status="">
      <cloudIDMapping cloudProviderId="vpc-0f61afe17568417c8"/>
    </cloudBrownfield>
    <cloudCidr name="cidr1" addr="40.0.0.0/16" primary="yes" />
  </cloudCtxProfile>
</fvTenant>
```

この例では、次のポストに示すように、EPG が VRF vrf1 を介してブラウンフィールドクラウドコンテキストプロファイルに関連付けられていることに注意してください。

```
<fvTenant name="unmanagedTenant1">
  <fvCtx name="vrf1" />
  <cloudApp name="ap3">
    <cloudEPg name="epg3">
      <cloudRsCloudEPgCtx tnFvCtxName="vrf1"/>
      <fvRsProv tnVzBrCPName="contract4"/>
      <cloudEPSelector name="EP_SEL1" matchExpression="IP=='40.0.0.0/24'" status="" />
    </cloudEPg>
  </cloudApp>
</fvTenant>
```

## AWS でのブラウンフィールド VPC の残りの構成の完了

次の手順では、AWS の残りの構成を完了します。次のセクションでは、AWS でこれらの残りの構成を完了するための一般的な手順と構成例を示しますが、構成が異なる場合があることに注意してください。

### 始める前に

次の手順を実行する前に、次の手順を実行する前に、必要なすべての設定が完了していることを確認します。

- [GUI を使用したアンマネージド \(ブラウンフィールド\) クラウドコンテキストプロファイルの作成 \(13 ページ\)](#)

- GUIを使用したブラウフィールドクラウド コンテキスト プロファイルと関連付けられた EPG の作成 (23 ページ)
- GUIを使用した EPG 間のコントラクトの作成 (26 ページ)

## 手順

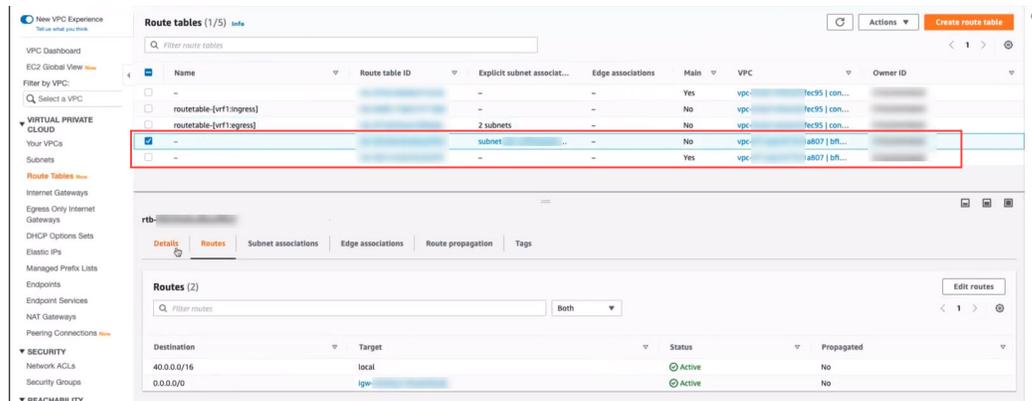
**ステップ 1** AWS ポータルで、[ルート テーブル (Route Tables)] ページに移動します。

[ルート テーブル (Route tables)] ページが表示され、構成済みのルート テーブルがすべて表示されます。

**ステップ 2** ブラウフィールド VPC 用に作成された 2 つのルート テーブルを見つけます。

VPC 列でブラウフィールド VPC の VPC ID を持つエントリを探し、ブラウフィールド VPC 用に作成された 2 つのルート テーブルを見つけます。

たとえば、ブラウフィールド VPC の VPC ID が ...a807 で終わることがわかっている場合は、次の図に示すように、[VPC] 列でその VPC ID を持つ 2 つのルート テーブルを見つけます。



**ステップ 3** 2 つのルート テーブルのどちらがサブネットのルート テーブルであるかを判別します。

ルートを編集するには、サブネットルート テーブルを選択する必要があります。サブネットルート テーブルは、次の識別子を使用して見つけることができます。

- 明示的なサブネット関連付けの列には、サブネットのエントリがあります。
- メイン列には No というエントリがあります。

**ステップ 4** サブネットのルート テーブルの横にあるボックスをクリックしてブラウフィールドルート テーブルを選択し、[ルートの編集 (Edit routes)] をクリックします。

[ルートの編集 (Edit routes)] ウィンドウが表示されます。

**ステップ 5** [ルートを追加 (Add routes)] をクリックします。

追加ルートの新しい行が表示されます。

**ステップ6** [宛先 (Destination) ]フィールドに、トランジットゲートウェイのCIDRを入力します。

**ステップ7** [ターゲット (Target) ]フィールドで、[トランジットゲートウェイ (Transit Gateway) ]を選択します。

前に作成したトランジットゲートウェイアタッチメントが自動的に読み込まれます。これは、ブラウンフィールド (アンマネージド) VPCとインフラストラクチャトランジットゲートウェイの間で、プロセスの一部として作成されたトランジットゲートウェイアタッチメントです。Cisco Cloud APIC管理対象外 (ブラウンフィールド) クラウドコンテキストプロファイルの作成 (12 ページ)

**ステップ8** [変更の保存 (Save Changes) ]をクリックします。

このルートテーブルの詳細ウィンドウが表示されます。

**ステップ9** トランジットゲートウェイを介して新しいルートが使用可能であることを確認します。

a) AWS ポータルで、[トランジットゲートウェイルートテーブル (Transit Gateway Route Tables) ] ページに移動します。

[トランジットゲートウェイルートテーブル (Transit gateway route tables) ] ページが表示され、トランジットゲートウェイ用に構成されたすべてのルートテーブルが表示されます。ルートテーブルのうち2つは2つのVRFに関連付ける必要があります。一方のルートテーブルはグリーンフィールドVPCのVRFに関連付けられ、もう一方のルートテーブルはブラウンフィールドVPCのVRFに関連付けられます。

b) これら2つのVRF関連ルートテーブルの最初の左側にあるボックスをクリックします。

このルートテーブルの詳細ペインが表示されます。

c) [ルート (Routes) ] タブをクリックし、使用したエントリと一致するCIDR列のエントリが、[ルート状態 (Route state) ] 列のアクティブ状態で表示されていることを確認します。ステップ6 (31 ページ)

d) 2つのVRF関連のルートテーブルの2番目についてこれらの手順を繰り返し、CIDR列の同じエントリが、2番目のVRF関連のルートテーブルの[ルート状態 (Route state) ] 列のアクティブ状態で表示されることを確認します。

**ステップ10** ブラウンフィールドVPCのセキュリティグループルールプログラミングを構成します。

Cisco Cloud APICは、ブラウンフィールドVPCのセキュリティグループルールプログラミングを構成しないため、AWSポータルから手動でこれらの構成を行う必要があります。

ブラウンフィールドVPCのセキュリティグループルールプログラミングの構成に使用できる情報については、次のAWSの記事を参照してください。

#### VPCのセキュリティグループ

以下は、ブラウンフィールドVPCのセキュリティグループルールプログラミングを構成する方法を示す構成例で、新しいエンドポイントを生成したり、既存のエンドポイントにセキュリティグループを適用したりできます。

たとえば、新しいエンドポイントを生成する場合：

a) AWSポータルで、[インスタンスの起動ウィザード (Launch Instance Wizard) ] を見つけて起動します。

- b) [インスタンスの詳細の構成 (Configure Instance Details)] ウィンドウが表示されるまで、[インスタンスの起動ウィザード (Launch Instance Wizard)] の [AMI の選択 (Choose AMI)] ウィンドウと [インスタンス タイプの選択 (Choose Instance Type)] ウィンドウをナビゲートします。
- c) [インスタンスの詳細の構成 (Configure Instance Details)] ウィンドウの [ネットワーク (Network)] フィールドで、ブラウフィールド VPC を選択します。
- d) セットアップに基づいて [インスタンスの詳細の構成 (Configure Instance Details)] の残りの構成を完了し、[次へ：ストレージの追加 (Next: Add Storage)] をクリックします。
- e) [セキュリティグループの構成 (Configure Security Group)] ウィンドウが表示されるまで、[ストレージの追加 (Add Storage)] および [タグの追加 (Add Tags)] ウィンドウの画面をナビゲートします。
- f) [セキュリティグループの構成 (Configure Security Group)] ウィンドウでセキュリティグループルールを手動で追加します。

[ルールの追加 (Add Rule)] をクリックして、セットアップに適切なセキュリティグループルールを追加します。

[インバウンドルール (Inbound rules)] には、グリーンフィールド CIDR が含まれます。

- g) セキュリティグループルールの追加が完了したら、[確認して起動 (Review and Launch)] をクリックします。
- h) [レビューと起動 (Review and Launch)] ウィンドウで情報を確認し、[起動 (Launch)] をクリックします。

構成したセキュリティグループルールに基づいて、残りの構成を完了します。

別の例として、既存のエンドポイントがあるとしてします。

- a) AWS ポータルの [ネットワークとセキュリティ (Network & Security)] で、[セキュリティグループ (Security Groups)] を見つけてクリックします。
- b) [セキュリティグループの作成 (Create security group)] をクリックします。
- c) [セキュリティグループの作成 (Create security group)] ウィンドウで必要な情報を入力します。

- [VPC] フィールドで、ブラウフィールド VPC を選択します。

- このウィンドウの [インバウンドルール (Inbound rules)] および [アウトバウンドルール (Outbound rules)] 領域の下にある [ルールの追加 (Add Rule)] をクリックして、セットアップに適切なセキュリティグループルールを追加します。

[インバウンドルール (Inbound rules)] には、グリーンフィールド CIDR が含まれます。

- d) 必要なセキュリティグループルールの追加が完了したら、ページの下部にある [セキュリティグループの作成 (Create security group)] をクリックします。
- e) [インスタンス (Instances)] ページに移動します。
- f) エンドポイントを選択し、[アクション (Actions)]、[セキュリティ (Actions)]、[セキュリティグループの変更 (Change security groups)] の順にクリックします。 > >
- g) [セキュリティグループの変更 (Change security groups)] ウィンドウで、作成したセキュリティグループを追加し、[保存 (Save)] をクリックします。



**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



#### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。